FACULTY OF LAWS

SYLLABUS

FOR

P.G. DIPLOMA IN CYBER LAW & INFORMATION SECURITY

(Semester I & II)

SESSION: 2013-14

GURU NANAK DEV UNIVERSITY AMRITSAR

(ii) Subject to change in the syllabi at any time.
Please visit the University website time to time.

Eligibility Criteria:

Students of following Streams are eligible for this scheme with minimum of 50% marks (aggregate)

M.Sc. (CS,IT,N/W)
M.Sc in Physics, Math(With B.Sc in C.S and Eco))
L.L.B,L.LM
MBA (I.T)
MCA

Objective of the Course:
Success in any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given way to express criminal tendencies. The course has been specifically designed to understand, explore, and acquire a critical knowledge in Cyber law. To develop competencies for dealing with frauds and deceptions To be conversant with the social and intellectual property issues in Cyberspace. To explore the legal and policy developments in Cyberspace To develop the understanding of relationships between commerce and cyberspace To give learners in depth knowledge of Information Technology Act and legal frame work of Right to privacy, Data Security and Data Protection.

Duration: **1 year (2 semesters)**

SEMESTER WISE BREAK UP OF COURSES

First Semester:

S.No.	Subject	Theory	Lab	Hours
PG–101	Soft Skill	60	40	4 ½ Hrs
PG–102	Advanced Programming in C Language	60	40	4 ½ Hrs
PG–103	International Treaties, IPR and Cyber World	60	40	4 ½ Hrs
PG–104	Network Technology	60	40	4 ½ Hrs
PG–105	Cyber Crime IT and Other Acts	100		4 ½ Hrs
PG–106	Lab based on Basic Computer Skill	--	100	4 ½ Hrs

Second Semester:

S.No.	Subject	Theory	Lab	Hours
PG–201	Information Security, Crime and Investigation	60	40	4 ½ Hrs
PG–202	Cyber Law and Forensics Issues	60	40	4 ½ Hrs
PG–203	Web Technology	60	40	4 ½ Hrs
PG–204	Cryptography	60	40	4 ½ Hrs
PG–205	Computer Security, Audit & Assurance	100	--	4 ½ Hrs
PG–206	Project/Dissertation	100	--	4 ½ Hrs

PG DIPLOMA IN CYBER LAW & INFORMATION SECURITY
(SEMESTER–I)

PG–101: SOFT SKILLS

Lectures: 4½ Hrs. / Week
(4 T, 2 P)

M.Marks: 100
Theory: 60 Marks
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Self Development and Assessment: Self-Assessment, Self-Awareness, Perceptions and Attitudes, Values and Belief Systems, Personal Goal Setting, Career Planning, Self-Esteem, Building of Self Confidence

Unit–II

Verbal and Nonverbal Spoken Communications: Includes planning, preparation, delivery and feedback and assessment of activities like: Public speaking, Group Discussions, Oral Presentation skills, Perfect interview, Listening and observation skills, Body Language, Use of presentation graphics, Use of presentation aids, study Communication Barriers

Unit–III

Written Communications: Technical Writing – Technical reports, Project Proposals, Brochures, Newsletters, Technical Articles, Technical Manuals, Official / Business Correspondence: Business Letters, Memos, Progress Reports, Minutes of Meeting, Event Reporting, Use of Style, Grammar and Vocabulary for effective Technical writing, Use of Tools, Guidelines for technical Writing, Publishing

Unit–IV

Ethics and Etiquettes: Business Ethics, Etiquettes in social as well as office settings, E-mail etiquettes, Telephone Etiquettes, Engineering ethics, and ethics as an IT Professional, Civic Sense

Unit–V

Leadership and Interpersonal Communications: Leaders – their skills, roles, and responsibilities, Vision, Empowering, delegation, motivating others, organizational skills, Problem Solving and conflict management, team building, interpersonal skills. Organizing and conducting meetings, decision making, giving support

Unit–VI

Other Skills – Managing Time, Meditation, Understanding roles of Engineer's and their responsibilities, Exposure to work environment and culture in today's job places, improving personal memory, Study skills that include Rapid Reading, Notes Taking, Complex problem solving and creativity.

Reference Books:

1. Shiv Khera, "You Can Win" – Macmillan Books – 2003 Revised Edition.
2. Stephen Covey, "7 Habits of Highly Effective People"
3. John Collin, "Perfect Presentation", Video Arts MARSHAL.
4. Jenny Rogers, "Effective Interviews", Video Arts MARSHAL.
5. Raman, Sharma, "Technical Communications", OXFORD. Sharon Gerson, Steven Gerson, Technical Writing Process and Product", Pearson Education Asia, LPE Third Edition.
6. R Sharma, K. Mohan, "Business Correspondence and Report Writing", Tata McGrawHill,

PG–102: ADVANCED PROGRAMMING IN C LANGUAGE

Lectures: 4½ Hrs. / Week **M.Marks: 100**
(4 T, 2P) **Theory: 60 Marks**
Practial: 40 marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Overview of Programming concepts and C Basics:

Unit–II

Arrays and Strings: Single and Multi Dimensional arrays – Strings, String manipulations.
Pointers: Definition and use of pointers, address operator, pointer variable, pointer arithmetic, arrays of pointers, passing arrays to functions, pointers and functions, constant pointers, pointers to functions. Dynamic Memory **Allocation:** Library functions for Dynamic Memory Allocation, Dynamic multi-dimension arrays.

Unit–III

Structures: Declaring and using Structures, operations on Structures, arrays of structures, user defined data type, nested structures, "sizeof" operator, pointer to structure, Self referencing structures.
Unions: Difference between Unions and structures, operations on a Union, Scope of a union, Bit fields, Bit-wise and shift operators, command-line arguments, using argc, agrv and env variables, Storage classifiers: auto, static, register and external, compiling multi-file programs.
Macro Preprocessor: macro definitions, macro with parameters and conditional compiling.

Unit–IV

Basic Architecture of 8086/88, Addressing modes, segments, General purpose registers, Inside the CPU and memory, ROM Startup, basic, BIOS, extension routines, Disk Basics, Keyboard Basics, Interaction with hardware through C.

Unit–V

Files: Introduction, File Structure, File handling functions, File types, Error Handling, Low level file I/O, redirection and piping, Writing C Programs using files with high level and low level I/O and BIOS system calls. Concept of IVT, IVR and TSR's

Reference Books:

1. Dromy R., “How to solve it by computer”, Prentice Hall of India

2. S. Kochan, “Programming in C”, CBS Publishers and Distributors.

3. Pointers in C by Y Kanetkar, BPB Publishers

4. Yashwant Kanetkar “Let us C” BPB Publishers

5. Microprocessors by Avtar Singh

Practical: C Programs, Designing GUI using ANSI C, Interrupt Handling Programs, Mouse Programming.

PG–103: INTERNATIONAL TREATIES, IPR & CYBER WORLD

Lectures: 4½ Hrs. / Week
(4 T, 2 P)

M.Marks: 100
Theory: 60 Marks
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Introduction:
Introduction to Intellectual Property Rights
GATT & WTO, WIPO, TRIPS, Berne convention , Universal Copyright Convention, WIPO Copyright Treaty (WCT), Copyright Act 1957, Trades Marks Act, 1999, Definition, Breach and remedies.
Data Protection:

(i) Principles of Data Protection
(ii) Jurisdictional issues
(iii) Retention of e- records
(iv) Transactional Data Flow and International Controls

Unit–II

Open source software, Copy left, Undisclosed Information/ Trade Secret, Reverse Engineering Anti Circumvention laws, Specific Problems/ Areas, Linking, Framing, Metatagging Domain names, Cyber squatting, ICANN, Uniform Domain Name Dispute Resolution Policy.

Unit–III

International Treaties:
PCT, PLT, SPLT, Washington Treaty

Unit–IV

Patents:
Indian Patent Act, Definitions breach and remedies, Application of Patents to information technology Patents for computer software, Patents for electronic commerce, Patent and Patentability criteria in India, US, EPC, Japan, China, Singapore etc, Various national and International Patent classifications , Identifying classes of a draft patent, Patent Search using internet Patent websites of US_PTO, EPC, WIPO and other countries, Distinctions in claims, Vetting of patents, IT related patents in India, Undesired patents.

Unit–V

Definitions Semiconductor Integrated Circuits and Layout Design Act 2000, Definitions breach and remedies.

Practical: Case Studies related to IPR Cyber world and Electronic Commerce.

PG–104: NETWORK TECHNOLOGY

Lectures: 4½ Hrs/ Week **M.Marks: 100**
(4 T, 2P) **Theory: 60 Marks**
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Basic Theory:
Types of Networks, Peer-Peer Networks, Client/Server Networks, Host Terminal Network, Wireless Network, Wi-Fi Network, Virtual Private Network, Internet, Intranet.
Protocols:
Network Protocols, TCP/IP (IP4 & IP6), SPX/IPX, NETBEUI, Tunneling Protocols PPTP, L2TP, IP SEC, Application Protocols FTP, TELNET, HTTP, HTTPS, Mail Protocols, SMTP, POP, IMAP, Frame Formats & Standards, Ethernet 802.2, 802.3, Wireless 802.11a, 802.11g.

Unit–II

Network Components & Topologies:
Connectivity Components, Connectors RG45,CAT Cables, Ethernet Cards, HUBS, Switches, Routers Modems, Dial-up Modem , ISDN Modem, DSL(Cable) Modem, Using Ethernet Card for Accessing , Internet, Bus, Star, Ring and Wireless loop topologies.

Unit–III

Microsoft Network Technology:
Features of Microsoft Windows Server 2003.
Server Roles, File and print server, Web server and Mail server Web application services, Terminal server Remote access and VPN server, DNS, Dynamic Host Configuration, Protocol server, and Windows Internet Naming Service.
Features of various types of Servers.
Standard Server, Enterprise Server, Data Center Server, Web Server, Small Business Server.

LINUX Network Technology:
Concepts:
Linux File System and structure, Default directories, Network services, http, https, ftp, nfs, BOOTTP, DHCP, Basic commands, User Management, File Management, Process Management, Printer and Device Management, Network Management, Package Management

Unit–IV

Introduction Medium access control - Telecommunication systems - Satellite systems – Broadcast systems.
Adhoc Networks Characteristics - Performance issues - Routing in mobile hosts.

Unit–V

Network issues Mobile IP - DHCP - Mobile transport layer - Indirect TCP - Snooping TCP - Mobile TCP - Transmission / timeout freezing - Selective retransmission - Transaction oriented TCP.

Reference Books:

1. Introduction to Networking Rechard McMohan Tata McGraw Hill Publication.

2. Computer Network Fundamentals and application – R S Rajesh Vikas Publication.

3. Unleashed Windows 2003 Server – Todd Brown & Chris Miller Techmedia SAMS Publication.

4. Microsoft Windows 2000 Professional – Paul Cassel Techmedia SAMS Publication.

5. J. Schiller, Mobile Communications, Addison Wesley, 2000.

6. William C.Y. Lee, Mobile Communication Design Fundamentals, John Wiley, 1993.

Practical: Installing and configuring various services of Server 2003 and Linux.

PG–105: CYBER CRIME IT AND OTHER ACTS

Lectures: 4½ Hrs. / Week **Theory: 100 Marks**

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Cyber Crimes:
Meaning Nature & Classification, kinds of Cyber Crimes.

Unit–II

Jurisdictional Issues:
Definition: Jurisdiction to prescribe/Legislative Jurisdiction; Jurisdiction to adjudicate to enforce; Cyber Jurisdiction in Civil, Criminal & International Cases.

Unit–III

Laws & Acts:
Unicitral Model Law, Information Technology Act, 2000, Relevant Rules Notifications, Information Technology (Amendment) Act, 2008.

Unit–IV

Cyber Slacker:
Ethics and Etiquette in Cyber World
Potential Liability of Intermediaries, Service Providers and Network Users, Cyber Stalking.

Unit–V

Intellectual Property: Piracy, Insider Threat, Corporate Espionage, Monitoring– Eavesdropping, Traffic Analysis, Surveillance. Defensive Information Warfare Telecommunication Security; Computer Network Security, Computer Break-Ins, Cryptographic Techniques, Steganography;

Relevant Court Case:
Pune Citibank Mphasis Call Center Fraud
Bazee.com case
State of Tamil Nadu Vs. Suhas Katti
The bank NSP Case
SMC Pneumatics (India) Pvt. Ltd. V. Jogesh Kwatra
Parliament Attack Case
Andhra Pradesh Tax case
Sony.sambandh.com case
Nasscom Vs. Ajay Sood & others
Infinity e-Search BPO Case

PG–106: Lab based on Basic Computer Skill

Lectures: 4½ Hrs. / Week **Practical: 100 Marks**

Internal and external Commands of DOS.

Working and Handling of Widows environment.

Basic operation of MS Word, PowerPoint and Excel.

Working with SQL.

Working with internet like browsing, e-mailing, chatting.

PG–201: INFORMATION SECURITY, CRIME AND INVESTIGATION

Lectures: 4½ Hrs/ Week
(4 T, 2P)

M.Marks: 100
Theory: 60
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

The State of threats against computers, and networked systems, Overview of computer Security and why they fail Vulnerability assessment, managing firewalls and VPNs, Overview of Instruction Detection and Intrusion prevention Network and host-based IDS. Classes of attackers, Kids/ hackers/ sophisticated groups, automated: Drones, Worms and Viruses A general IDS model and taxonomy.

Unit–II

Information security risk analysis fundamentals Importance of physical security and biometrics controls for protecting information systems assets, Security considerations for the mobile work force, Network security perspectives, networking and digital communications (overview only), security of wireless networks.

Unit–III

Security models and frameworks and standards through introduction to the ISO 27001, SSE-CMM (systems security engineering – capability maturity model), COBIT (Control Objectives for Information and related technologies) and the Sarbanes-Oxley Act (SOX) and SAS 70 (statement on auditing standards)**,** Privacy Fundamentals, business practices, impact on data privacy, technological impact on data privacy, privacy issues in web services and applications based on web services.

Unit–IV

Internet/Computer Demographics: Computer/network user statistics; Computer crime statistics. Types of Computer and Internet Crime: Types of crimes involving computers; Computer crimes; Network crimes; Criminals, hackers, and crackers
Investigations: The investigation life cycle; Legal methods to obtain the computer; Jurisdictions and agencies; Internet investigations (e-mail, IRC, chat rooms, etc.); IP addresses and domain names; Investigative methods, Digital Evidence
Evidence Collection: Working with ISPs and telephone companies; Examining computer, server, and network logs; Anonymous services.

Unit–V

Introduction to Information System Security, Offensive and Defensive Information Warfare:
Cyber Crime: Fraud and Abuse; National Security, Offensive Information Warfare; Privacy Rights, Ethics, Censorship, Harassment;
Prevention Techniques: Access Control, Misuse Detection; Vulnerability Monitoring, Security Policy, Risk Management, Incident Handling; Law Enforcement and Cyber Crime, Emerging Concept in Cyber Crime.

Text/ References Books:

1. Information Systems Security Management by Nina S. Godbole (Wiley India Pvt.Ltd.)
2. Security Engineering by Ross Anderson
3. Information Security Management Handbook by Harold Tpton & Micki Krause (Auerbach Publications)
4. Network Security Essentials: Applications and Standards W. Stallings (Pearson Education)
5. Security Planning & Disaster Recovery by Eric Maiwald and William Sieglein (Tata McGraw-Hill)
6. M. Erbschloe, J. R. Vacca: Information Warfare: How to Survive Cyber Attacks (McGraw-Hili Prof. 2001.)
7. Jones, G. L. Kovacich, and P. G. Luzwick: Global Information Warfare: How Business, Governments, and Others Achieve Objectives and Attain Competitive Advantages (CRC Press, 2002.)
8. D. Denning: Information Warfare and Security (Addison Wesley) 1998.

Practical: Case Studies based on Cyber crime and investigation process.

PG–202: CYBER LAW AND FORENSICS ISSUES

Lectures: 4½ Hrs/ Week
(4 T, 2 P)

M.Marks: 100
Theory: 60 Marks
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Introduction to Computer Hardware Forencics, Granularity, Sandboxing and Proof-carrying code, Hardware protection, Other technical Attacks.

Unit–II

Multilevel and Multilateral Security Multilevel Security, Multilateral Security
Monitoring Systems Introduction, Alarms, Prepayment Masters.

Unit–III

Internet Security:
Computer Security and Threats, Hacking, Cracking, sneaking, Viruses, Trojan Horses, malicious code, Worms and Logic Bombs.
Network attack and Defence Most Common Attacks, Scripts Kiddies and Packaged Defense.

Unit–IV

Introduction (Biometric Security):
Authentication and Biometrics Overview, How Authentication Technologies Work How Biometrics Work, Where can Biometrics be applied
Types of Biometrics:
Fingerprint and Hand Geometry, Facial and Voice Recognition,Eye Biometrics: Iris and Retina Scanning , Signature Recognition and Keystroke Dynamics, Esoteric Biometrics

Unit–V

Issues Involving Biometrics: Biometric Liveness Testing, Biometrics in Large-Scale Systems, Biometric Standards Biometric Testing and Evaluation Privacy, Policy, and Legal Concerns Raised by Biometrics, Biometrics and Privacy, Legal Considerations of Government Use of Biometrics Case Study The Law and Private-Sector Use of Biometrics Review of Selected Biometrics Programs Government and Military Programs, Private–Sector Programs

Text/ References:

1. Cyber Laws – Singh Yatindra
2. Cyber Crime – Bansal S.K.
3. Cyber Law, E-commerce & M-Commerce – Ahmand Tabrez.
4. Handbook of Cyber and E–Commerce Laws – Bakshi P.M. & Suri R.K.
5. Ashbourn, J.: Practical Biometrics – From Aspiration to Implementation, Springer Verlag, 2004.
6. Bolle, R.M., Connell, J.H., Pankanti, S., Ratha, N.K., Senior, AW.: Guide to Biometrics, Springer Verlag, 2004.
7. Chirillo, J., Blaul, S.: Implementing Biometric Security, Wiley Publishing, 2003.
8. Nanavati, S., Thieme, M., Nanavati, R: Biometrics–Identity Verification in a Networked World, Wiley Publishing, 2002.
9. Woodward, J.D., Orlans, N.M., Higgins, P.T.: Biometrics–Identity Assurance in the Information Age, McGraw-Hill Osborne Media, 2002.

Practical: Case Studies based on Cyber Forensic Issues

PG–203: WEB TECHNOLOGY

Lectures: 4½ Hrs/ Week
(4 T, 2 P)

M.Marks: 100
Theory: 60 Marks
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

INTRODUCTION:
A brief introduction to Internet, WWW, Web Browser, Web Server, Uniform Resource Locater, Repeators, Bridges, Routers, Gateways, Internet Topology, HTTP, *TCP/IP,* IP, ARP, RARP, ICMP, Web pages: types and issues, concept of Tier, Frames, Forms, Plugins.

Unit–II

HTML AND DHTML:
Origin and Evolution of HTML, Basic Syntax, Standard, HTML Document Structure, Basic text Formatting, Images, Hypertext Links, Lists, Tables, Frames, Forms, DHTML.

Unit–III

UNIT 3: JAVASCRIPT:
Qverview, Object Orientation and Java Script, General Syntactic Characterestic, Primitive Operations and Expressions, Control Statements, Constuctors, Functions, Pattern Matching.

Unit–IV

JAVASCRIPT AND HTML DOCUMENT:
The JAVA script Execution Environment, The Document Object Model, Element Accession JAVA script, Event Handling, Dynamic Documents with JAVA script.

Unit–V

INTRODUCTION TO WEB SERVER AND SERVELETS:
WEB Server Operation, General Server Characteristics, Overview Of Serve lets, Servelets Details, JAVA Servelets, Serve lets API, Serve Lifecycle, HTML Aware Serve lets, HTML Specific Servelets.

Text/ References:

1. Achyut Godbole, Atul Kahate ,"Web Technology ",Tata Mc Grew Hill.
2. Programming World Wide Web: Robert W Sebesta Pearson Education.

Practical: Based on HTML and Java Script and Serverlets.

PG–204: CRYPTOGRAPHY

Lectures: 4½ Hrs/ Week
(4 T, 2 P)

M.Marks: 100
Theory: 60 Marks
Practical: 40 Marks

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Foundations of Cryptography and Security: Ciphers and Secret Messages, Security Attacks and Services.
Mathematical Tools for Cryptography: Substitutions and Permutations, Modular Arithmetic, Polynomial Arithmetic.

Unit–II

Conventional Symmetric Encryption Algorithms: Theory of Block Cipher Design, Feistel Cipher Network Structures, DES and Triple DES, Modes of Operation (ECB,CBC, OFB,CFB), Strength (or Not) of DES.
Modern Symmetric Encryption Algorithms: IDEA, CAST, Blowfish, Twofish, RC2, RC5, Rijndael (AES), Key Distribution.

Unit–III

Stream Ciphers and Pseudo Random Numbers: Pseudo random sequences, Linear Congruential Generators, Cryptographic Generators, Design of Stream Cipher, One Time Pad Public Key Cryptography: Prime Numbers and Testing for Primality, Factoring Large Numbers, RSA, Diffie-Hellman, EIGamal, Key Exchange Algorithms, Public-Key Cryptography Standards **Hashes and Message Digests**: Message Authentication, MD5, SHA, RIPEMD, HMAC Digital Signatures, Certificates, User Authentication: Digital Signature Standard (DSS and DSA), Security Handshake Pitfalls, Elliptic Curve Cryptosystems.

Unit–IV

Authentication of Systems: Kerberos V4 and V5, X.509 Authentication Service Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME, X.400 IP and Web Security, IPSec and Virtual Private Networks, Secure Sockets and Transport Layer (SSL and TLS).

Unit–V

Electronic Commerce Security: Electronic Payment Systems, Secure Electronic Transaction (SET), Cyber Cash, iKey Protocols, Ecash (DigiCash) Digital Watermarking and Steganography.

Text/ References:

1. C. Y. Hsiung, Elementary Theory of Numbers.
2. W. Stallings, Cryptography and Network Security Principles and Practice, 2/e.
3. Charlie Kaufman, Radia Perlman, Network Security.
4. Wenbo Mao, Modern Cryptography: Theory and Practice, Prentice Hall, 2004.
5. Richard A. Mollin, An Introduction to Cryptography, Chapman and Hall/CRC, 2001.

Practical: Based on implementation of various algorithms.

PG 205: COMPUTER SECURITY, AUDIT AND ASSURANCE

Lectures: 4½ Hrs/ Week **Theory: 100 Marks**

Instructions for Paper Setter:

1. The Paper setter is required to set eight questions in all that is each unit must contain at least one question and the candidate be required to attempt any five questions out of these eight questions.
2. The Papers which are of 100 marks will contain 20 marks for each question and the papers which are of 60 marks will contain 12 marks for each question.

Unit–I

Introduction to computer based systems and their Security, Policy standards and Organization, Information Classification and Security awareness.
Information System Audit and Assurance - An Overview, Determination of policy (ies) and the degree of assurance required from controls, Information Security Management System (ISMS), Audit and review of ISMS Internal Control and Information System Audit information Security Governance and Assurance and Audit Security Controls, Systems Assurance and Control (SAC), Systems Audit ability and Control (SAC) reports, Control Objectives for Information and Related Technologies

Unit–II

Attack and Threat Analysis, various types of Attacks and Threats and their Analysis on Security. Security Management techniques, The policy led approach, Infrastructure assessments, System assessments, Business case assessments for improvements. Study of various tools and techniques available for Security risk analysis. Security Controls, Physical Security, Virtual Private Networks (VPNs), IPsec, Access Controls, Identification and Authentication Techniques, Managed Firewalls, Data Monitoring Software, Email Security, and Cryptology.

Unit–III

Security Policies and Procedures, An investigation into the types of policies and procedures you need to consider, How to formulate your IT Security Policy, IT Policy standards, Creating, implementing, and managing controls and monitoring mechanisms, as well as other important security policies and procedures.

Unit–IV

IT Security Audits, Systematic technical assessments of how well the security policy is working, personal interviewing, vulnerability scanning, examining operating system settings, analysis of network shares, review of firewall management, physical security, penetration test techniques, reviewing audit logs, look at encryption used, and view documentation from any changes to systems or software.

Unit–V

Audit tools, enterprise Computing, Report Card, OS/400i Series, PS Audit, Auditor's Computer Audit etc. Management of Information Assurance, The identification of technical and human factors in prevention, detection and reporting of computer and information system weaknesses; the vulnerability, threat, risk, and impact on information assurance; and the significance of these factors on an organization's intellectual property and viability.

Text/ References:

1. Fischer & Jordan, "Security Analysis and Portfolio Management", 6th Ed., Prentice Hall of India, Ed., 2005.
2. Rajaraman, "Introduction to Information technology", Prentice Hall of India, Ed., 2005.
3. Edwards, et al., "The essence of Information Systems, Prentice Hall of India, 2nd Ed., 2005.
4. Murdick, Ross & Claggett, "Information Systems for Modern Management", Prentice Hall of India, 3rd Ed., 2005.
5. A. Blyth and G. L. Kovacich, "Information Assurance", Springer, 2005.

PG–206: PROJECT/DISSERTATION

Lectures: 4 Hrs/ Week **Theory: 100 Marks**

Project Based on Network Security and information Security.